1 Aug 88

MEMORANDUM OF AGREEMENT

This Office of Information Resources (OIR)/Office of Information Technology (OIT) Memorandum of Agreement (MOA) addresses issues pertaining to the transition of SAFE from OIT to OIR and identifies OIR/OIT responsibilities as they relate to the development, maintenance, and operation of the SAFE systems. The agreements are as follows:

1. Architecture

a. Current

(1) Hardware and System Software (VM, MVS): OIT shall have responsibility for the installation, maintenance and configuration of all hardware and operating systems within the SAFE computer systems (classified and unclassified).

(2) SAFE Application Software: OIR shall have responsibility for the development and maintenance of all CIA SAFE Application software within the SAFE systems.

(3) AIM: OIT shall have responsibility for the development and maintenance of all AIM software as AIM serves a larger population than SAFE. However, recognizing that both offices want to eventually divorce AIM from the SAFE applications software and ensure that no change to SAFE or AIM shall be detrimental to either, an Interface Control Document (ICD) shall be established to contain description and formats of software requiring joint (OIT and OIR) control. ICD items shall initially include the SAFE Terminal Manager, software currently known as the AIM Userside, and the AIM Applications Program Interface (API) when designed. OIR shall have responsibility for developing the ICD with OIT participation.

(4) SAFE/AIM Terminal Manager: OIR shall have responsibility for the development and maintenance of the software currently known as the SAFE/AIM Terminal Manager. As previously stated above, this software shall be under joint control.

(5) Data Base Management System: OIR shall have responsibility for the development and maintenance of the INQUIRE data base management system within the CIA SAFE systems.

(6) Currency of Operating Systems/AIM: OIT and OIR agree to maintain currency of Operating Systems/AIM and SAFE applications software.

b. Future

(1) OIR shall have responsibility for the future architecture of the SAFE application which includes:

- Hardware
- System Software
- Data Base
- Application Code
- User Interface
- Distributed Processing Capability
- SAFE Terminal Manager
- AIM Userside Software

(2) OIR shall coordinate changes in the architectures and applications with OIT to ensure that system availability, performance, levels of service, can be maintained. OIT shall make recommendations to OIR for future SAFE architectures.

2. Performance Measurement/Evaluation

a. System Performance: OIT shall have responsibility for the measurement, evaluation and reporting of system performance and capacity within the SAFE computer environment (unclassified and classified systems).

b. Application Performance: OIR shall have responsibility for the measurement, evaluation and reporting of the SAFE application within the SAFE computer environment.

c. Both offices are committed to performance enhancements that maintain and/or improve the OIT level of service standards. OIT shall provide operating system and AIM performance enhancements, while OIR shall provide SAFE application software performance enhancements.

3. Configuration Management

a. The OIT Services Management Board shall retain overall responsibility for the configuration control of the centralized computer

and communications hardware and system software for all OIT systems, including SAFE. However, OIR, through the SAFE CCB, must approve all configuration changes to all SAFE computer systems (including classified and unclassified systems) prior to their implementation.

b. Application Software: OIR shall have responsibility for approving authority through the SAFE Configuration Control Board (CCB) for all application software changes to the SAFE computer systems.

c. AIM Software: OIT shall have responsibility for approving authority through the AIM CCB for all AIM software. However, for those items in the SAFE/AIM ICD, approval from both the OIR SAFE CCB and the OIT AIM CCB is necessary before the work can start.

d. Boards:

(1) Configuration Control Boards: OIR shall chair the CIA SAFE CCB. OIT shall provide a voting member to the CIA SAFE CCB. OIT shall chair the AIM CCB. OIR shall provide a voting member to the AIM CCB.

(2) Engineering Review Boards: The CIA SAFE ERB and AIM ERB shall be organized similarly to the CIA SAFE and AIM CCBs. However, the AIM ERB is a technical, non-voting forum.

(3) Operations Review Board: OIR shall chair the CIA SAFE ORB. OIT shall continue to participate in the CIA SAFE ORB.

4. Operations

a. Operation of SAFE Computer Systems: OIT shall have responsibility for providing computer operations and maintenance support for the SAFE computer environment. The Operations Scheduling Panel (OSP) chaired by OIT shall continue with overall responsibility for scheduling hardware and systems software changes to all OIT systems including the SAFE computer systems. OIR shall provide a representative to the OSP, replacing the current CSPO representative. The OIR representative shall have the right to delay a proposed change to the SAFE configuration when intelligence needs conflict with the proposed OIT schedules.

b. Data Base Control Center: OIT shall have responsibility for providing 24 hours/day, 7 days/week support for the CIA SAFE classified and unclassified systems.

c. Consolidated Applications Branch: OIT shall have responsibility for providing support for the CIA SAFE production and test systems, including 24 hours/day, 7 days/week on-call support.

5. SAFE Unclassified System

a. Administration: OIR shall have responsibility for the SAFE VMU ADP Control Officer.

b. Maintenance Support: OIT shall have responsibility for providing computer operations and maintenance support to SAFE contractor sites, DIA and the SAFE unclassified environment.

c. OIT and OIR shall have responsibility for developing a plan to secure the CIA SAFE unclassified system to support continued development and testing of CIA SAFE applications. OIR shall have overall responsibility for developing the plan.

6. Contracts

a. OIT shall have responsibility for providing mainframe computer hardware/commercial software licensing acquisition support for the SAFE computer environment. OIR shall continue to fund the above support.

b. OIT is committed to awarding letter contracts to INFODATA, LOGICON, TRW, and HADRON on or before 1 August 1988. OIT shall definitize these letter contracts by early December 1988. In addition, OIT shall complete the source selection, to include ACRB approval, and award the contract for system integration and engineering support NLT 1 October 1988. Subsequent administration of the above contracts shall be assumed by OIR.

7. Communications

a. OIT shall have responsibility for the operations, maintenance, and planning of the telecommunications network connected to the SAFE computer configuration.

b. OIT shall have responsibility for the licensing and/or secure external telecommunication link to the CIA SAFE computer configuration using OIR funds as appropriate.

APPROVE:

STAT

Director of Information Resources

28 JUL 1988
Date

STAT

Director of Information Technology

1 AUG 1988
Date